REMARKS

In an Office Action dated September 7, 2006, the Examiner rejected claims 3, 9-12 and 15-18 under 35 U.S.C. §102(e) as anticipated by McCulligh (US 6,643,784).

Applicants have amended all independent claims herein to clarify the nature of their invention. Specifically, the claims have been amended to recite that there are a plurality of sets of validity requirements corresponding to different password-protected resources, the password string for a common password being simultaneously verified against each of said sets. As amended, the claims are patentable over the cited art.

Applicants' specification discloses a system for verifying passwords, the system having multiple features. Among the features disclosed in applicants' specification is the ability to verify a common password, i.e. a single password string which is used to access multiple different password-protected resources. As will be appreciated, there is generally a set of requirements associated with any password used to access a password protected resource. Such requirements may include, e.g., a maximum and minimum number of characters in a password string, which characters are considered valid and invalid, requirements that sequential characters be dissimilar, and so forth. The set of requirements is often defined independently for each password-protected resource, so that a string satisfying the set of requirements for accessing one password-protected resource might fail to satisfy the set of requirements for accessing a different password-protected resource.

With the proliferation of password-protected resources, a user may wish to use a common password to access more than one resource in order to reduce the number of passwords the user must memorize. However, it is difficult for a user to keep track of all the rules for each of multiple different password-protected resources, and to assure that any chosen common password

satisfies all applicable requirements. If the user attempts to verify a common password serially against multiple sets of requirements corresponding to different respective password-protected resources, he may find that the common password is acceptable to some resources before determining that it is unacceptable to one resource, and then have to start all over again. This can be difficult and frustrating to the user.

In accordance with applicant's claimed invention, the common password string is simultaneously verified against multiple sets of validity requirements, each set corresponding to a respective password-protected resource, at least some sets being different.

McCulligh, cited by the Examiner, discloses a system which verifies compliance of a password with a set of rules expressing a single set of validity requirements, i.e. a set of requirements for any valid password to access a single password-protected resource. Applicants' claim 3 previously recited verifying the password string "against validity requirements of more than one password-protected resource". In his rejection, the Examiner appears to take the position that the recited "validity requirements of more than one password-protected resource" reads on multiple rules (validity requirements plural) defining access requirements for a single password-protected resource. The Examiner's reasoning is that either the "resource" is a rule, or that the same set of rules defines a password for accessing multiple resources (as a system, which contains multiple resources).

In order to clarify the nature of the invention, applicants have amended the independent claims herein. Applicants' representative claim 3, as amended, recites:

3. A computer system, said computer system comprising:
a bus;
a central processing unit;
memory, said memory being connected to said central processing unit via said bus; and
a password validation mechanism for verifying a *single common password string for accessing a plurality of password-protected resources*, each said password-protected resource having a single corresponding set of validity requirements of a plurality of sets of validity requirements, *each said set of validity requirements independently defining requirements of a valid password string for accessing the corresponding password-protected resource, said password protection mechanism verifying simultaneous compliance of a single common password string with each said set of validity requirements* of said plurality of sets of validity requirements, said plurality of sets of validity requirements including a first set of validity requirements for a password string for accessing a first password-protected resource and a second set of validity requirements for a password string for accessing a second password-protected resource different from said first password-protected resource, said *first set of validity requirements being different from said second set of validity requirements*, said password validation mechanism providing simultaneous feedback to a user regarding validity of a said single common password string against each said set of said plurality of sets of validity requirements. [emphasis added]

The remaining independent claims, while not identical in scope, contain limitations analogous to the italicized language above.

As amended, claim 3 recites that a password is for *accessing* a password-protected resource, and that a set of validity requirements defines requirements of a valid password string for accessing the password protected resource. Applicant submits that the amended language disposes of any interpretation that a password-protected resource is a "rule"; as used in the claims, the password-protected resource is something that is *accessed* using the password.

Furthermore, as recited in the claims, each password-protected resource has a *corresponding set of validity requirements* which define the requirements of a valid password, there being multiple such sets. Finally, the claims recite that at least some of the sets are different. Therefore, although the term "password-protected resource" standing alone could read

on multiple resources of a system which is accessed by a single password, in this case all the resources have the same set of validity requirements, i.e. the set corresponding to the system. Thus the limitation that at least some of the sets are different is not met.

McCulligh shows verifying a *single* set of rules for accessing a single password-protected resource. While applicants appreciate the Examiner's argument that a single password-protected resource may accessed by a password may give the user access to a hierarchy of resources, hence multiple password-protected resources, in this case there is not a separate set of rules to be verified for accessing each of the multiple resources, as recited in applicants' amended claims.

For all of the reasons above stated, the claims as amended are not anticipated by *McCulligh*. Nor are the claims obvious over *McCulligh*. *McCulligh* is concerned with verifying a password against a single unitary set of rules. There is nothing that would suggest simultaneous verification of a common password against multiple different sets of rules corresponding to different resources, as disclosed and claimed by applicant.

Applicants have added new dependent claims 19-22. Dependent claims 19, 20 and 22 recite the feature of using a different visual cue, such as a different color, for each resource (set of requirements). Dependent claim 21 further recites the independence of the sets of validity requirements, i.e. it is possible to satisfy each set without satisfying the other. These features are further not taught or suggested by *McCulligh*.

In view of the foregoing, applicant submits that the claims are now in condition for allowance, and respectfully requests reconsideration and allowance of all claims. In addition, the

Examiner is encouraged to contact applicant's attorney by telephone if there are outstanding issues left to be resolved to place this case in condition for allowance.

Respectfully submitted,

BRIAN J. CRAGUN, et al.

By:_____
Roy W. Truelson
Registration No. 34,265

Telephone: (507) 202-8725